Official will notify the contractor and provide guidance for the review process. The contractor may review, comment on, rebut, or supplement past performance reports within 30 calendar days of the evaluation. If the contractor would like a meeting to discuss the CPAR, a written request must be forwarded to the Assessing Official within seven calendar days from notification of the evaluation. All past performance reports must be finalized in the Contractor Performance Assessment Reporting System (CPARS) annually.

SECTION C – STATEMENT OF WORK

C.1 OVERVIEW

The Army National Guard (ARNG) Personnel (G1) is responsible for creating, managing, and executing all manpower and personnel plans, programs, and policies across all the ARNG Directorates. The Reserve Component Manpower System-Guard (RCMS-G) and the Strength Maintenance Management System (SMMS) are used to support and enhance the ARNG G1 decision-making process. Most data input to this system is raw data that indicates the status of Reserve Component personnel and the changes that have occurred to the force during the current reporting period. SMMS/RCMS-G processes these data elements and converts them into useful information for the users. The output generated may take on many forms, such as a graphical output showing grade and year-of-service profiles, a budget book showing the cost of the manpower program over the Future Years Defense Programs (FYDP), or statistics showing personnel readiness during mobilization.

SMMS/RCMS-G provides its users with the ability to readily access the personnel data, extract and integrate the data from multiple sources, refine and improve the data, and make it available to decision makers in a form that makes trends and key issues apparent for making critical Guard-wide decisions.

The services required to maintain SMMS/RCMS-G include project management, operations and maintenance, and data operations. The operations and maintenance are tasks related to system, database, and web server maintenance, service desk, cyber security monitoring, defect identification, tracking, and resolution, and change and configuration management support, continuity of operations and disaster recovery. Included in data operations are tasks related to include data processing, data reprocessing, mainframe operations, and maintenance of system interfaces with approximately 40 external systems. Additionally, analytical support includes report generation and ad hoc queries provides decision support to the ARNG G1 and liaison support is required across all ARNG G1 divisions in order to ensure that the program is aware of developing requirements.

Currently, there are three (3) significant requirements that are essential to maintaining SMMS/RCMS-G as a resource for the ARNG.

1) First, the SMMS/RCMS-G systems uses an obsolete software development kit (Adobe Flex) which uses Adobe Flash to make browser-based software perform similar to desktop software. Adobe Flash reached end of life on 31 December 2020 and both previous vendors were unable to transition the system fully from Adobe Flex. The

Authorizing Official for the ARNG has accepted the risk to allow the continued use of Adobe Flash beyond the end-of-life support with the implementation of a number of risk mitigation steps. However, this exception is only extended through August 2021 and requires conversion of all remaining Adobe Flash modules to be completed by this deadline. Approximately 20 SMMS and RCMS-G modules have been identified for conversion from Adobe Flash to HTML5. As of March 2021, migration work has begun with the most critical and complex of the modules, to include the Director's Personnel Readiness Overview (DPRO), Guard Incentive Management System (GIMS), Automated Unit Vacancy System (AUVS), E-Tracker (HRP and HRH versions), Retention Management System (RMS), and Record Brief. The remainder of the portfolio have only had minimal work or analysis completed for the Adobe Flash to HTML conversion, but must be completed during this bridge contract award period.

2) Second, the servers that support the SMMS/RCMS-G systems require improved security and capabilities. As of February 2021 RCMS-G servers are running Microsoft SQL Server 2008 and SMMS server MS SQL 2014. Upgrading to MS SQL Server 2016 will reduce data vulnerability by providing a data encryption solution through role-based access control, row and column level security. This solution will allow robust data queries within multiple sources/environments while reducing maintenance requirements especially if part of a Cloud computing service.

3) Third, there are significant changes pending in the inbound data set received from the Integrated Personnel and Pay System – Army (IPPS-A) with their release 3 (R3) in December 2021. The ARNG has already transitioned to IPPS-A's second release in March 2020, but the change in the inbound data from R3 will likely require a substantial retooling of procedures designed to process the data into the G1 Data Warehouse.

C.1.1 PURPOSE

The purpose of this requirement is to provide services for SMMS and RCMS-G; adhere to cyber security requirements; and maintain the operational readiness of all applications, modules, and interfaces. SMMS and RCMS-G must complete SQL upgrades, comply with DoD and industry security protocols, integrate new IPPS-A data and they must be maintained to facilitate transition out at the end of this contract.

C.1.2 AGENCY MISSION

To support the ARNG G1 mission, the SMMS/RCMS-G suite of applications and modules were developed to provide ARNG action officers and senior leaders with critical manpower information needed to enhance their decision-making process. SMMS/RCMS-G aggregates data from multiple authoritative data sources and presents results in the form of user information, such as reports, dashboards, or data files, which are delivered to authorized locations, or presented via Web portal.

C.2 SCOPE

The SMMS/RCMS-G suite is used to access, gather, and present manpower readiness data to ARNG decision makers. This requirement includes the operations, maintenance, data operations,

and analytical support for the SMMS/RCMS-G system and its users as well as making changes to the system to ensure compatibility with evolving technologies. In the performance of this contract, ARNG expects the contractor to provide innovative solutions that bring technical and operational improvements to the ARNG and its SMMS/RCMS-G users and customers. In providing services to SMMS/RCMS-G, the contractor shall coordinate its efforts with a number of other contractors and government organizations and maintain agreements with those organizational entities.

The scope of this contract includes the following:

1. Maintaining the operational readiness of the SMMS/RCMS-G applications, modules, and interfaces;

2. Maintaining the operating system (OS) of the SMMS/RCMS-G servers in the Primary environment and associated Continuity of Operations Plan (COOP) environment;

3. Supporting data operations by providing ongoing management of data feeds, maintenance of SMMS/RCMS-G metrics, and the processing of production data;

4. Providing changes to SMMS/RCMS-G analytical functions;

5. Providing project management and execution of all changes to the SMMS/RCMS-G applications, modules and interfaces, including the integration of selected ARNG G1 systems into the SMMS/RCMS-G environments;

6. Producing, updating, and maintaining the Business Process Reengineering (BPR), Department of Defense (DoD) Architecture Framework (DoDAF), and Business Enterprise Architecture (BEA) documents for all changes to the SMMS/RCMS-G suite;

7. Identifying and eliminating vulnerabilities to SMMS/RCMS-G and;

8. Achieving and maintaining information assurance and accreditation of the SMMS/RCMS-G systems in accordance with (IAW) DoD and federal standards (to include the Contact Pre-Qualification Processing System [CPPS], which supports lead generation from 1-800-GO-GUARD.COM). CPPS is administered by another source, IO Studios, but is included within the SMMS/RCMS-G accreditation boundary. The contractor shall purchase software licenses in order to fulfill the requirements of this solicitation. Software must be procured through the Army's Computer Hardware and Enterprise Services and Support (CHESS) contract, or other appropriate source. The TPOC must approve all purchases and sources in writing.

C.3 CURRENT ENVIRONMENT

The current environment is outlined in Section J, Attachment B.

C.4 OBJECTIVE

The overall objective of this requirement is to update all current software and data processes through a highly flexible and agile process that results in:

1. Sunset RCMS-G and migrate enduring RCMS-G capabilities into the SMMS
2. Incorporate Army HR data changes driven by IPPS-A, AIE, and other Army system modernization efforts into a streamlined and single data warehouse eliminating the need to process data separately for SMMS and RCMS-G that provide real time or close to real time data updates
3. Migrate to a Cloud based hosting environment to include a full spectrum SecDevOps SDLC (may be completed concurrently with objective 1 – RCMS-G sunset)
4. Maximize the efficiencies of the systems low code data driven architecture to increase system capabilities and flexibilities to drive change and produce actionable information

C.5 TASKS

C.5.0 TRANSITION

The contractor shall update the draft Transition-In Plan provided with its proposal and provide a final Transition-In Plan as required in Section F. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities shall be completed prior to transition-in POP completion.

Transition-in shall require coordination with the incumbent contractor for acceptance of the project. The contractor shall perform a joint inventory of all Government-furnished equipment (GFE) with the incumbent contractor and the TPOC or Property Book Officer. All discrepancies and problems shall be noted and submitted to the CO, CS, COR, and TPOC for resolution. The contractor shall inventory all GFE listed on DA Form 3161. The contractor shall have all key personnel available at the contractor award date, and all critical staff in place within 15 days after contract award. At the beginning of phase-in, the contractor shall also certify to the CO, CS, COR or TPOC, that all of the contractor's employees meet the training criteria as specified in Sections H.2.2 through H.5.

The key transition objectives for the transition of the SMMS/RCMS-G services to the TO awardee during the transition-in period are to:

1. Minimize transition impact to the user community;

2. Ensure no breaks in service availability;

3. Maintain existing service quality and performance levels;

4. Ensure a transparent and seamless transition;

5. Ensure that the IT security posture during transition is maintained at current levels without creating gaps and/or vulnerabilities.

6. Assume full system responsibility and be prepared to process all data on time meeting satisfactory or higher SLA standards.

The contractor shall execute the Incoming Transition Plan in a manner that positions the contractor to successfully assume responsibility for maintaining operational readiness of the SMMS/RCMS-G systems. At a minimum, SMMS/RCMS-G support includes:

1. Standing up the facility that meet the requirements presented in the SOW;

2. Hiring, training and obtaining required security clearances, certifications, and system-level access for all staff;

3. Transferring all knowledge required to operate and maintain the environment and to provide user support through the service desk; and

4. Establishing operational relationships with other organizations involved in the operations.

5. Ensuring a fully operational software development environment is in place and critical technical support personnel have all required access.

The contractor shall manage and perform all tasks required to transition operational support from the incumbent contractor.

The incoming contractor must understand that the incumbent's primary responsibility is to maintain operational capabilities of the SMMS/RCMS-G Suite during the transition period.

Therefore, the contractor shall not assume the incumbent staff will be available to provide dedicated or extensive assistance. It is the responsibility of the contractor to: obtain access to the operational systems, review existing materials to gain an understanding of the current operations and present a comprehensive plan for moving equipment, if needed, in a manner that minimizes disruption to ongoing operations. The contractor shall work with the TPOC to obtain this information. The TPOC will not dictate the approach, but must approve all plans.

The contractor shall understand that the SMMS/RCMS-G systems and applications along with their interfaces have been custom developed over many years utilizing a variety of software languages (including but not limited to: Adobe Flash, ASP.Net, HTML5, Javascript) this includes an off-the-shelf software solution called the UPTick Enterprise Software Solution. The UPTick implementation provides a data driven framework that allows the government a highly configurable low code environment consisting of applications that are META data configurations to produce fast reliable changes to the required configuration.

C.5.0.1 COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government TPOC. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss system access, management, security issues, travel authorization, and reporting procedures. At a minimum, the attendees shall include contractor key personnel, representatives from the directorates, other relevant Government personnel, and the CO, CS, COR, and TPOC. NLT five days after award the contractor will schedule the Kick-Off Meeting and deliver a draft Kick-Off Meeting Agenda for review and approval by the CO prior to finalization (Section F, Deliverable 1)

At least three days prior to the Kick-Off Meeting the contractor shall deliver the final Kick-Off Meeting Agenda (Section F, Deliverable 2). The agenda shall include at a minimum the following topics/deliverables:

a. Points of Contact (POC) for all parties;

b. Personnel discussion (i.e., roles and responsibilities and lines of communication between the contractor and Government);

c. Staffing plan status;

d. Updated Transition-In Plan and discussion (Section F, Deliverable 17);

e. Security discussion and requirements, i.e., building access, badges, Common Access Cards (CACs), telework agreements and limitations;

f. Invoicing requirements; and

g. Updated Baseline Quality Control Plan (QCP) (Section F, Deliverable 14).

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present at the meeting. The contractor shall draft and provide a Kick-Off Meeting Minutes Report documenting the Kick-Off Meeting discussion and any action items. (Section F, Deliverable 3)

Within 5 business days after the Kick-Off Meeting, the contractor shall submit completed system and system privileged access requests for all key personnel and any other staff that is identified by the contractor PM as critical to a successful transition. The contractor must work directly with all agencies responsible for granting required access and own the process of obtaining access. The contractor shall be responsible for ensuring that all personnel requiring access are in compliance with DoDD 8140 baseline certifications for the access they are requesting. The SMMS/RCMS-G PMO will support the contractor's efforts in obtaining access. Failure to obtain the required access will not relieve the contractor from any SOW tasks. A list of all individuals that require elevated/privileged access and those critical to the success of transition will be reported along with the key personnel status at least weekly during transition. Weekly Transition Report (Section F, Deliverable 4)

C.5.0.2 REQUIRED TASKS FOR TRANSITION

Facility: The contractor shall establish the operational and support facility, which will house all efforts associated with the technical requirements in this SOW. The proposed facility must meet the minimum requirements. See Section H.

C.5.0.2.1 KNOWLEDGE AND EQUIPMENT TRANSFER

Knowledge and Access: The contractor shall provide a weekly report of data processing, critical access status, equipment transfer, and environment inventory. Weekly Transition Report (Section F, Deliverable 4)

The contractor shall:

1. Develop and execute a Transition-In Plan (Section F, Deliverable 18);

2. Conduct an inventory of GFE and IT assets;

3. Establish management processes and controls necessary to support the transition process;

4. Inventory and verify all software titles and license keys settings necessary to operate and maintain the SMMS/RCMS-G systems and environments;

5. Inventory all source code, stored procedures, development and administrative tools, configuration settings, etc. necessary to operate and maintain the SMMS/RCMS-G systems and environments;

6. Gain access to and establish an understanding of all Enterprise Mission Assurance Support Service (eMASS) and the various controls, inherited controls, and associated artifacts;

7. Assume responsibility for moving GFE equipment from the current SMMS/RCMS-G service providers to the contractor's facility; and

8. Clean up the ticket data and transition tickets to the new ticketing system.

9. System environment access and control of software development operations.

10. Establish and demonstrate the ability to host virtual meetings using the ARNG selected medium. Currently the ARNG utilizes the Army ".cvr" version of Microsoft Teams and plans to transition to a CAC enabled O365 version of Microsoft Teams.

11. Observe data processing and review Data Processing Guide (DPG) documentation

C.5.0.3 SPECIFIC TRANSITION-IN REQUIREMENTS:

The contractor shall develop and execute a Transition-In Plan (Section F, Deliverable 18) that includes at a minimum:

1. Specific tasks to be performed and the resources assigned to them;

2. Task dependencies and relationships;

3. Proposed task duration; and

4. Major milestones.

The transition schedule shall be documented within the Incoming Transition Plan. At a minimum, the set of tasks shall include:

1. Personnel actions;

2. Hiring, obtaining/verifying clearance and certifications;

3. Accounts – requesting appropriate accounts from the Government (This process can take in excess of 30 days for new accounts to be provisioned and is the sole responsibility of the contractor to ensure government procedures are followed and system access is granted);

4. Training (including any required certifications and SMMS/RCMS-G specific training such as Metadata manager programming);

5. Schedule shall include milestones for percentage of staff ready for operations and maintenance (O&M) duties;

6. Facility. This section shall address progress towards outfitting the contractor's facility including subcontracts, leases, environmental issues, safety and security, etc. in the implementation of their transition strategy;

7. ARNG domain knowledge transfer;

8. Readiness reviews demonstrating the capability to operate and maintain the systems and environments.

The contractor shall schedule and conduct weekly status meetings to report and review progress of the transition (Section F, Deliverable 5)

Within the transition-in period responsibilities, the contractor shall demonstrate readiness to proceed prior to Assumption of Operational Responsibility (AOR). The ARNG will review the level to which the contractor was able to accomplish the transitional tasks. The contractor shall complete the following within the transition period in order to proceed with the task order:

1. The contractor shall demonstrate ability to take over administrative management of all SMMS/RCMS-G elements outlined in this SOW.

2. Demonstrate operational readiness of the contractor's facility, including:

    a) Completely outfitted physical office space for all of the contractor's personnel;
    b) Temporary private office and meeting space for the ARNG personnel;
    c) Service Desk space;
    d) Telephone system supporting the Service Desk in a manner that supports SLAs outlined in this solicitation;
    e) Physical access security; and
    f) Connectivity to SMMS/RCMS-G and associated networks and environments.

3. Demonstrate functionality of the ticketing system.

4. Demonstrate that the contractor staff has the certifications required to operate the ARNG's system management elements as outlined in this SOW.

5. Demonstrate that the contractor's staff understands established ARNG policies and procedures. See Attachment R for applicable DoD and Army directives, instructions and regulations.

6. Secure all user privileges and access needed to conduct the support services of this solicitation, if the contractor is relying on incumbent capture new/updated accounts must also be obtained for those employees. Access is tied to the contract and incumbent contractors will lose access once their contract ends.

7. Demonstrate successful execution of (20) daily, (4) weekly, and (1) monthly processing activities as needed to fulfill the support services of this solicitation.

8. Successfully support data processing during the transition period to include one End of Month (EOM) processing period.

C.5.0.4 SMMS/RCMS-G Data Processing Guide

The contractor observes all data processing during the transition period and compares actions performed to the actions described in the DPG. The contractor shall annotate and document all additional information required to successfully complete data processing in the data processing guide delta report (Section F, Deliverable 6).

C.5.1 TASK 1 – PROGRAM MANAGEMENT

The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW).

C.5.1.1 PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide a Monthly Status Report (Section F, Deliverable 7). The MSR shall include the following:

a. Activities during the reporting period by tasks (including, ongoing activities, new activities, activities completed, count of releases by category, and progress to date on all activities). Each section shall start with a brief description of the task.

b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.

c. Notification/information about any revoked or expired contractor personnel security clearances.

d. Government actions required.

e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each) This includes a release schedule with the high-level requirements that will be completed by module in each of the next three-monthly releases and what was released in the last actual monthly release.

f. Cyber Security compliance depicting the required and completed scans and all vulnerabilities and risks identified

g. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).

h. Accumulated invoiced cost for each CLIN up to the previous month.

i. Projected cost of each CLIN for the current month.

C.5.1.2 CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) shall convene a monthly Technical Status Meeting with the CO, CS, COR, TPOC, and any other necessary Government stakeholders (Section F, Deliverable 8). The purpose of the meetings is to ensure all stakeholders are informed of the monthly activities and MSR, SLA performance measurements review, and to provide an opportunity to identify other activities and establish priorities and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items to the CO, CS, COR, and TPOC within 5 business days after the meeting (Section F, Deliverable 9). These meeting

minutes shall include all priorities, identified problems and any recommended courses of action, opportunities and recommended courses of action, decisions made, and due out action items. Any nonconformance to any SLA or PRS must also be annotated with the reason for nonconformance and when the nonconformance will be brought back to a minimally acceptable level of conformance.

C.5.1.3 PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a draft PMP for TPOC/COR review (Section F, Deliverable 10). The final PMP shall incorporate TPOC/COR comments approved by the TPOC/COR. (Section F, Deliverable 11).

The PMP shall:

a. Describe the proposed management approach;

b. Contain detailed Standard Operating Procedures (SOPs) for all tasks;

c. Include milestones, tasks, and subtasks required in this TO;

d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations;

e. Describe in detail the contractor's approach to risk management under this TO including the transition in;

f. Describe in detail the software release and configuration planning schedule (Most modules/applications are currently on a monthly release cycle, however releases that contain only metadata changes are typically more frequent).

g. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government; and

h. Include the contractor's Baseline QCP.

C.5.1.4 UPDATE THE PROJECT MANAGEMENT PLAN

The PMP is an evolutionary document that shall be updated annually at a minimum. The contractor shall work from the latest Government-approved version of the PMP and update the PMP within 30 days of a substantial change (Section F, Deliverable 12).

C.5.1.5 TRAVEL REQUEST AND PREPARE TRIP REPORTS

The contractor shall submit a Travel Request (TR) for each individual participant. All TRs shall at a minimum include the information below in this section required for Trip Report. All TRs shall be reviewed and approved by the TPOC prior to participant travel.

The contractor shall submit Trip Reports to the TPOC, not later than (NLT) five business days after completion of a trip for all long-distance travel. Long distance travel is defined as travel

over 50 miles outside of the Washington, DC commuting area. Local travel will not be reimbursed. Travel to the Washington D.C. area for employees that are approved to telework in the best interest of the government must do so at the contractor's expense, unless a special exemption is approved by the TPOC and there are available funds. Long Distance Travel for telework employees beyond the 50-mile radius of their normal place of duty is authorized per JFTR to locations other than the Washington D.C. metro area.

The Trip Report shall include the following information:

a. Name(s) and title(s) of personnel who traveled;

b. Dates of travel;

c. Destination(s);

d. Purpose of trip;

e. Cost of the trip;

f. Approval authority; and

g. Summary of events.

The contractor shall keep a summary of all long-distance travel, including but not limited to the name of the employee, location of travel, duration of trip, and Point of Contact (POC) at the travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained (Section F, Deliverable 13).

C.5.1.6 PROVIDE QUALITY CONTROL MANAGEMENT

The contractor shall develop and maintain an effective QCP to ensure services are performed in accordance with Section C. The contractor's QCP is the means by which it assures that the services performed complies with the requirements of the resulting task order. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services.

The contractor's QCP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QCP shall describe how the appropriate methodology integrates with the Government's requirements.

The QCP shall include the following:

1. Organization and resources. Organization chart and communication interfaces for all personnel performing Quality Control (QC) functions. Identification of the authority of the QCP manager to monitor and control functions, and to implement remedial and preventive actions;

2. Specific inspection techniques and methods tailored to each functional area;

3. Risk Identification and Remediation Plan; and

4. Procedures for corrective action.

The contractor shall update the QCP submitted with its proposal and then provide a final baseline QCP (Section F, Deliverable 15). The contractor shall periodically update the QCP as required when changes in program processes are identified (Section F, Deliverable 16).

C.5.1.7 QUALITY CONTROL RESPONSIBILITIES

The contractor's quality control team shall monitor and promote adherence to established SMMS/RCMS-G service levels and schedules by analyzing Performance Requirements Summary (PRS) data, as well as existing policies and procedures Quality Control Updates (Section F, Deliverable 15).

The contractor's quality control team shall:

1. Formulate and enforce internal work quality standards;
2. Ensure users are notified with service request ticket status and provide resolution (closing tickets);
3. Produce and provide performance reports;
4. Conduct periodic performance reviews to improve current operations;
5. Maintain statistical data in order to demonstrate performance trends;
6. Conduct independent quality assurance reviews of closed tickets to ensure they are managed properly;
7. Prepare training plans for the development of the staff and to improve service support;
8. Identify user training needs based on analysis of tickets;
9. Investigate report statistics and analysis as appropriate;
10. Investigate missed requirements and identify root causes for the non-compliance; and
11. Identify issues (technical, management, or otherwise) that prevent the contractor from meeting the Service Level Agreements (SLAs) and/or other operational goals.

C.5.1.8 OPSEC SOP/PLAN

The contractor shall develop an Operational Security (OPSEC) Standard Operating Procedure (SOP)/Plan and provide it to the TPOC and COR within 30 calendar days of contract kick-off meeting to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan shall include a process to identify the government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. The contractor shall implement OPSEC measures as required by the Government. In addition, the contractor shall identify an individual who will be an OPSEC

coordinator. The contractor shall ensure this individual becomes OPSEC Level II certified within 90 days of appointment as OPSEC coordinator in accordance with AR 530-1. Contractor shall provide a copy of the certification to the COR and TPOC NLT 15 days after completion (Section F, Deliverable 20).

C.5.1.9 STANDARD OPERATING POLICIES AND PROCEDURES

The contractor shall establish and maintain formalized Standard Operating Policies and Procedures (SOPs) and operational plans for each process that supports the operation and maintenance of SMMS/RCMS-G.

The contractor shall deliver these (new or updated) procedures for review and approval by the Government. Standard operating procedures include:

1. Service Desk and On-site Support; including ticket creation, updates and resolution;
2. Onboarding, account creation and provisioning;
3. Disaster Recovery Plan;
4. Continuity of Operations Plan (COOP) (Section F, Deliverable 27);
5. Crisis Communication Plan;
6. Cyber Incident Response Plan;
7. Backup, Archive, and Recovery;
8. Update Data Processing Guide (Section F, Deliverable 24);
9. OPSEC SOP/Plan (Section F, Deliverable 20);
10. Cloud Resource Management; and
11. Change Management Plan (Section F, Deliverable 30).

All SOPs shall be delivered to the Government within 60 days after contract award and the contractor shall brief the Government within five business days of the delivery (Section F, Deliverable 34) prior to acceptance of the SOP by the Government.

The contractor shall update these plans and procedures within 30 calendar days of identifying a change (Section F, Deliverable 35) and the Government reserves the right to reject an SOP if it does not meet the mission requirements. If rejected the contractor shall resubmit any rejected SOP within 10 business days for reconsideration.

C.5.1.10 SMMS/RCMS-G TRANSITION OUT

The Contractor shall develop a Draft Transition-out Plan (Section F, Deliverable 37). The Draft Transition-out Plan shall be delivered to the CO, COR, and TPOC and incorporate government feedback into a Final Transition-out Plan (Section F, Deliverable 38). In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. Points of contact.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel.
g. Schedules and milestones.
h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor and Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition out.

The contractor shall implement its Transition-Out Plan NLT four months prior to expiration of the TO.

The TPOC will notify the contractor of all outstanding requirements that shall be completed prior to task order expiration and the contractor shall:

Ensure that all information assets and related configuration information are up to date and available for the Government's review at least five months prior to the expiration of the task order; and

Phase 1: Ninety calendar days prior to the expiration of the task order, the incumbent contractor shall deliver to the Government images/VMs of the SMMS/RCMS-G development and test environments (development and test servers and workstations) with all associated tools, documents to include previous and source code:

1. Production: Images/VMs hosted at incumbent contractor site, related to current SMMS/RCMS-G production environment and solution files, team foundation server or any source code related to the application or sub-Applications;

2. Development: Images/VMs hosted at incumbent contractor site, used to develop SMMS/RCMS-G environment to include all production release version and solution files, team foundation server or any source code related to the application or sub-Applications;

3. Turn over all administrative access information, i.e., username and password to the ARNG at least 60 calendar days prior to the end of the contract;

4. Work with the incoming contractor in transitioning the operational support; and

5. Provide documentation and information as requested by the Government (the contractor shall deliver a copy of all current and relevant system documentation created during the contract).

Phase 2: The contractor in accordance with its phase-out plan shall develop and execute an approach to transition program knowledge to the government and incoming contractor. This approach includes but is not limited to SOPs, plans, information papers, and lessons learned. Knowledge transferred shall include backup and restoration procedures. The incumbent contractor is not responsible to train the incoming contractor, however the incumbent shall make all aspects of the contract available for observation of employees performing the tasks. This includes questions and answers as the incumbent is performing SOW tasks.

C.5.1.11 ENTERPRISE CONTRACTOR MANPOWER REPORTING APPLICATION (ECMRA)

The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site and delivered via email to the Technical Point in addition to GSA Assisted Services Shared Information System (ASSIST) Information Technology Support Services (ITSS) at portal.fas.gsa.gov. The secure data collection site is operated and maintained by the Office of the Assistant Secretary of the Army-Manpower & Reserve Affairs (ASA-M&RA). This task does not change the contract type basis.

Accounting for contractor Support: The contractor shall completely fill in all required data fields using the following web address: http://www.ecmra.mil/. Reporting inputs shall be for the labor executed during the period of performance during each Government fiscal year (FY), which runs from October 1 through September 30. Inputs shall be reported annually and are due NLT October 31 of each calendar year, beginning with 2021, (Section F, Deliverable 19). Contractors may direct questions to the help desk at http://www.ecmra.mil.

C.5.2 TASK 2 – DATA PROCESSING

The contractor shall utilize the Kimball Data Warehousing Methodology to support SMMS/RCMS-G data operations. Data Operations are foundational to the success of the entire program. Conducting these data operations requires flexibility to optimize the accuracy and frequency of all inbound and outbound data processing. Data processing often requires concurrent and dependent processing that cannot be accomplished during core business hours alone. The contractor shall provide a comprehensive data processing guide that provides a step-by-step guide to complete all data processing and preprocessing tasks. This document shall be updated as processes change, new feeds are added or deleted, and clarifying information is identified. This guide is intended to provide technical experts the ability to perform all duties required to successfully perform acceptable data processing; it is not intended to teach the technical skills needed to perform these data processing tasks. (Section F, Deliverable 22).

Data Pre-Processing: The purpose of data pre-processing tasks is to ensure that the date set files received by the SMMS/RCMS-G are valid and complete. ARNG defines “valid data” as data that conforms to the expected data characteristics as defined in the destination tables and does not deviate from the historical patterns.

The contractor shall:

1. Receive data from the external sources. Most interfaces require daily data updates. These interfaces are already established with automated processes (see Task 5 for Systems Interface Requirements);

2. Ensure that all expected data sources have delivered their data (via automated data feeds) by the time agreed-upon in the corresponding agreements;

3. Conduct pre-processing of external data feeds to ensure that record counts and file structures are consistent with previous data feeds as a quality control measure, repair and report abnormalities and raise alerts if it appears that any inconsistencies exist and establish new processes for quality control when existing quality control process are not already in place;

4. Load pre-processed data into the SMMS/RCMS-G production Data Warehouse; and

5. Provide the capability to store copies of verified source data in the staging SMMS/RCMS-G databases and store these data copies.

6. Identify and report all changes to inbound data formats, files not received, or non-conforming data received within 12 hours of identification (Data Processing Status Report Deliverable 22)

C.5.2.1 DATA PROCESSING

The purpose of data processing tasks is to ensure that the data set files received by the SMMS/RCMS-G are properly inserted into the existing SMMS/RCMS-G tables.

The contractor shall:

1. Create data sets for inclusion into the SMMS/RCMS-G data warehouse, by removing data duplications as identified by the system. Only data records that represent a change or new records shall be appended to a historical database for the life of the system thus supporting accurate backward and forward time series analysis and comparisons;

2. Load pre-processed data into the SMMS/RCMS-G production data warehouse; and

3. Close records that need to be closed based on the existence of updated records in the source data. SMMS/RCMS-G never replaces any records; rather old records are closed, and new records are inserted. For example, if a soldier is promoted, a new record with the

promotion information is inserted into the database and the old record is “closed” by populating “end date” of the previous rank

C.5.2.1.1 DATA PROCESSING ERROR RESOLUTION

As issues with the incoming data are identified, the contractor shall:

1. Identify and/or respond to inquiries of data abnormalities contained within SMMS/RCMS-G source data, especially as it relates to the historical data sources;

2. Identify and carry out corrective actions to resolve data abnormalities;

3. Create ad hoc reports using various tools including MS Excel, SQL and MS PowerPoint and other tools to communicate data issues with ARNG leadership and functional experts;

4. Create resolution methodologies that will minimize data anomalies and invalid or missing data; and

5. Report all data anomalies, concerns, failures, or other noteworthy events within 12 hours of identification and include remediation requirements and timelines (Data Processing Status Report Deliverable 22)

C.5.2.2 MAINFRAME OPERATIONS

In addition to data sources identified above, the SMMS/RCMS-G system processes data stored on a Pentagon mainframe. The Pentagon Mainframe exists as part of the Joint Service Provider Enclave and is a shared space with the Army Reserve. Some data is a shared incoming data feed containing USAR and ARNG data. The contractor shall develop a government approved Memorandum of Understanding (MOU) to conduct data sharing of incoming data to the Mainframe with any third-party vendors. The contractor shall perform data operations for these data sources that include the following tasks:

1. The contractor shall maintain a historical archive of source data files that reside on the Pentagon mainframe. On a frequent basis, the contractor shall copy data sets received from SMMS/RCMS-G interfaces to/from the Pentagon mainframe. A process for this bi-directional data push already exists.

2. The contractor shall provide connections to other systems. This applies primarily to a limited number of situations where the SMMS/RCMS-G interfaces do not provide their data sets directly to SMMS/RCMS-G; rather, these data sources send their data to the Pentagon mainframe and SMMS/RCMS-G pulls these data sources from the mainframe. An example of such an arrangement is the Defense Manpower Data Center (DMDC), which puts Defense Finance and Accounting Service (DFAS) data onto the Pentagon mainframe.

3. The contractor shall include Mainframe Operations in the Data Processing Status Report (Section F, Deliverable 22).

C.5.2.3 DATA PROCESSING DOCUMENTATION

The contractor conducts all data processing each period and compares actions performed to the actions described in the data processing guide (DPG). The contractor shall annotate and document all additional information required to successfully complete data processing in the data processing guide. (Update Data Processing Guide Deliverable 24).

C.5.3 TASK 3 - DATA OPERATIONS

The contractor shall utilize the Kimball Data Warehousing Methodology to support SMMS/RCMS-G data operations. Data Operations are foundational to the success of the entire program. Conducting these data operations requires flexibility to optimize the accuracy and frequency of all inbound and outbound data processing.

The contractor shall:

1. Maintain and change existing automated data quality control processes by verifying and validating anomalies;

2. Use historical information as the basis for conducting analyses to determine if the new data sets are within an acceptable range and meet expected characteristics;
3. Develop metrics using background statistics and linear regression analysis to determine the validity of the data;

4. Perform periodic data checks on the metrics to identify any data abnormalities;

5. Inspect abnormalities in the metrics to determine if the change is expected or might be signaling an anomaly that may exist;

6. Create data sets for inclusion into the SMMS/RCMS-G data stores by removing data duplications as identified by the system;

7. Create resolution methodologies that will minimize data anomalies and invalid or missing data;

8. Identify and carry out corrective actions to resolve data abnormalities and report abnormalities to user;

9. Inspect abnormalities in the metrics to determine if the change is expected or might be signaling an anomaly that may exist;

10. Maintain and change existing automated data quality control processes by verifying and validating anomalies; and

11. Perform periodic data checks on the metrics to identify any data abnormalities.

12. Report Data abnormalities (Data Processing Status Report Deliverable 22).

C.5.3.1 DATA REPROCESSING

Based on historical records, the ARNG anticipates that a small percentage of the data obtained from the external sources will have corruptions that cannot be identified using the standard check and data quality control processes discussed above. These issues are typically caused by mistakes introduced in the data feeds or data processing. When such issues are discovered, the contractor shall:

1. Work with the owner of the data source to create methods for identifying the corrupted elements in the SMMS/RCMS-G staging database and update the affected records to their correct values;

2. Rerun all standard checks and quality control processes and reload the updated data into the SMMS/RCMS-G data store following the data fixes to the staging area;

3. Keep historical records of all such events, including at minimum, information about the data source, issues, affected date range, fields, and steps taken to resolve the problem;

4. Evaluate these events for inclusion into the standard data verification and quality control processes; and

5. Deliver the results of this analysis and the details about each event to the ARNG as part of the Data Processing Status Report (Section F, Deliverable 22).

C.5.3.2 DATABASE(S) MAINTENANCE

The contractor shall manage the performance and availability of these SMMS/RCMS-G databases that comprise the SMMS/RCMS-G Suite data store. As of January 2021, the environment is comprised of Microsoft SQL 2008, 2012, and 2014. The contractor shall migrate any existing servers to the latest approved Microsoft SQL server database release prior to the existing SQL version causing a security vulnerability.

The structure and size of the SMMS/RCMS-G databases are the following:

DB Server Name	Capacity (GB)	DB Storage Used (GB)	Databases	Tables	# of SProcs
NGRCA4-RCMSDB01	7771	5380.82	66	10691	8484
NGRCA4-RCMSDB02	5047	2669.38	83	34974	14716
NGRCA4-RCMSDB03	9320	7060.51	27	13341	4264
NGRCA4-SMMSDB01*	11308	5939.08	87*	17102*	24568*
NGRCA4-SMMSDB02	19140.5	14206.68	65	19677	15265
NGRCA4-SMMSDB05	180	32.37	21	386	2739

***24 of the DBs, 4737 of the Tables, and 9906 of the Stored Procedures are for the Exercise environment;**

The environments shall include Development, Test/Staging, Exercise, and Production environments and may be expanded or decreased as necessary to meet SMMS/RCMS-G mission requirements.

The contractor shall monitor and resolve performance issues, data access and setup, monitor status of scheduled backups, coordinate and write processes for inbound and outbound data transfers, and create schedule to run and monitor all required Extracting, Transforming and Loading (ETL) processes.

The contractor shall be responsible for:

- Developing and maintaining replication processes to ensure accurate and available data in the various production environments;
- Providing ongoing coordination with software maintenance team(s) for tailored products, modules, and models database and best practices support;
- Assessing and improving the database performance, mod schema, manage indexes, produce roll up tables and views and alter speed indexes; and
- Monitoring data alerts and respond and resolve these issues.
- Reporting data discrepancies and improvement processes achieved in the monthly status report (reference C.5.1.2).
- Updating existing and adding new metadata utilizing the existing implemented open-source UPTick software to maintain the integrity of ARNG G1 manpower metrics and their relevance to supporting ARNG manpower analysis requirements.

- Modifying stored procedures to incorporate business logic as a result of customer driven changes to policy and practice.

- Providing a monthly Operational Health report (Section F, Deliverable 21). This report shall include:
    1. Capacity Management Statistics
    2. Successful VM/DB Backup Statistics
    3. System Security tasks required/accomplished
    4. System Patches required/accomplished
    5. Performance Tuning
    6. Availability
    7. All relevant statistics and explanations for suboptimal system health, to include a Plan of Action and Milestones (POAM) for all risks.

Outage Notification:

The contractor shall be responsible for:

1. Communicating information about known outages to the users and other support organizations;
2. Communicating scheduled maintenance notification at least 48 hours in advance; and
3. Communicating information about known issues and their anticipated resolution times.

The contractor shall ensure that its notification about unscheduled maintenance is posted no less than 15 minutes before the start of the maintenance.

The contractor shall submit an SMMS and RCMS-G System Operations and Maintenance Operational Health Report (Section F, Deliverable 21)

C.5.3.3 SYSTEM INTERFACES

The contractor shall establish and maintain the system interfaces with external modules, systems, applications, and databases. Approximately 40 interfaces exist between SMMS/RCMS-G and external systems. This task is inclusive of adding, modifying, and deleting system interfaces as well as adding, modifying, and deleting supporting system interface agreements.

An interface agreement is valid for one to three years or until a major change occurs. Interface agreements may be called a number of other names such as Interface System Agreement (ISA), Computer Matching Agreement (CMA), or Operational Level Agreement (OLA). Regardless of name, the interface agreement typically includes a background, authorities, security controls, roles, and responsibilities, signatory authorities, points of contact, technical instructions and data file layouts.

The contractor shall accomplish the following tasks:

- Change inbound/outbound interfaces to support technology changes, data changes and refreshment;

- Develop database schemas and tables to support interface changes;

- Populate new tables to support growing product lines within the RCMS-G database;

- Establish extracts of data to support requests for information from external systems;

- Ensure that all ISAs between RCMS-G and SMMS are properly implemented;

- Coordinate and work directly with all interface partners to ensure all required information is provided to support all agreements;

- Conduct meetings at least twice monthly with all pertinent parties for any existing or desired interface that is non-compliant with the terms of the ISA or any desired data source working toward an ISA. ISA Non-compliance report (Deliverable 39);

- The contractor shall utilize IPN and/or CSP provided Microsoft Structured Query Language (SQL) 2014 or greater and MySQL NetBackup agents to back up and restore Database Servers. Add new, modify existing, and delete obsolete interface agreements as required in the interface lifecycle; and

- Output: System Interface Agreement documents shall be archived approximately 40 times per year and shall be updated thirty days prior to the TO expiration. (Section F, Deliverable 23).

C.5.4 TASK 4 – CYBER SECURITY AND COMPLIANCE

The contractor shall work with Cyber Security Service Providers (CSSP) and other 3rd parties to monitor and respond to cyber threats.

The contractor shall:

1. Support 3rd party Security Control Assessments and Validations (SCA-V) by providing all supporting documentation and explanation of artifacts;

2. Perform vulnerability assessments in order to prepare for and in support of systems Security Control Assessments and Validation events;

3. Perform RMF or current DoD standards assessments of the SMMS/RCMS-G;

4. Perform source code and executable scans of the SMMS/RCMS-G system and ensure that the system meets all NIST and DoD security requirements;

5. Monitor and respond to Information Operations Condition (INFOCON) Levels to comply with the SD 527-1 or current standard required baseline. When the INFOCON level is

elevated, document the level change, the needed readiness activities, the completion of those activities, and any issue associated with complying with the INFOCON required steps;

6. Review and identify recommendations for Chief Technology Officers (CTOs), Execution Orders (EXORDS), including necessary waiver requests and POAMS and deploy guidance and procedures for all INFOCON levels and transitions between them;

7. Support implementation of the emerging cyber warfare doctrines, as required;

8. Update documentation and systems such as e-MASS to reflect system compliance with security controls, architecture, etc.;

9. Ensure the environment maintains accreditation under the Risk Management Framework (RMF) accreditation and all other requirements to continue receiving a Tenant in Good Standing Certificate. Authorization to Operate, and/or an IATT;

10. Contractor shall ensure that the Army HBSS, SCCM and Antivirus clients are installed and functional; and

11. Coordinate and follow through with all government agencies to ensure all system security and compliance requirements remain compliant and in good standing with DoD policy and guidance

12. Develop and maintain a MOU with the ARNG G6 that clearly delineates all Responsibilities, Accountability, Consulted partners, and Informational Awareness required for all security and compliance tasks

13. Plan, Identify, and Coordinate all security and compliance tasks and be responsible for ensuring all requirements are accomplished without system interruptions or limitations.

14. Output: The contractor shall provide an in-process review of Cyber Security and Compliance to include a resolution POAM during each monthly technical status meeting (Reference C.5.1.2).

C.5.4.1 SMMS/RCMS-G SECURITY SUPPORT AND USER ACCESS

The contractor shall ensure that all access to the SMMS/RCMS-G environment is CAC enabled. The contractor shall ensure that records are tied to the CAC login of the User entering the information in order to send system emails related to the particular record and auditability. The contractor shall implement an enterprise approach to roles and permissions management encompassing all modules, data, and web pages tools. The contractor shall implement single sign on capability for all modules.

C.5.4.2 SECURITY COMPLIANCE

The contractor shall maintain the SMMS/RCMS-G environment to meet all DoD system security standards and system accreditation standards as defined by DoD. Assessing Security and Privacy Controls in Federal Information Systems and Organizations is the current standard for selecting security controls in order to meet the Risk Management Framework (RMF) guidelines and all other requirements to continue receiving an Authorization to Operate (ATO) as appropriate.

SMMS and RCMS-G have an RMF categorization of Medium-Medium-Medium.

Security Controls are inherited from Common Control Providers (CCP) and the Army Policy Record.

The contractor is responsible for Implementing Security Controls, Assessing Security Controls, preparing for System Authorization events, and Monitoring Security Controls on a continuous basis.

The contractor shall ensure security controls selections are updated in order to ensure the system is updated appropriately to reflect DoD Accreditation and security standards. The contractor will ensure at a minimum that SMMS/RCMS-G meets the National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) and Federal Information Security Management Act (FISMA) guidelines set forth in the latest versions of the following documents which are available electronically under DoD government websites:

- NIST SP 800-53
- NIST Special Publication 800-53A Rev 4 (or current revision)
- FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems
- NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347
- NIST 800-129 Guide for Security-Focused Configuration Management of Information Systems
- NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems
- FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- DoDI 5000.2, Operation of the Defense Acquisition Systems

The contractor shall document both system security processes and any security incident or threat in the security section of the Program Management Plan. The contractor shall comply with DoD SOP requirements for compromised data breach as listed DoDD 5400.11-R (DoD Privacy Program) and relevant DoDI for policies and required actions.

The support in this area includes the following tasks:

1. Ensuring SMMS/RCMS-G application is programmed according to DISA Security Technical Implementation Guidelines (STIGs), SRG, and will run in an environment and on servers that are STIG/Unified Gold Master (UGM) compliant;

2. Validating configurations with an approved Security Content Automation Protocol (SCAP) scanner and provide scan results as eMASS artifacts and provided as requested;

3. Performing vulnerability scans and reviews to identify all patches and updates;

4. Providing automated daily vulnerability assessment and reporting based on asset inventory;
5. Automatically scanning the environment, source code, and stored procedures to identify and remediate vulnerabilities;

6. Automatically generating service tickets for detected vulnerabilities;

7. Aggressively mitigating vulnerabilities to prevent loss of capability, performance, or information, agency block, or other quarantine and/or user access limitations;
8. Providing the security-related support for patch management to include: Testing all security patches provided by the industry and the DoD to ensure they do not have negative impact on the operational systems;

9. Reviewing waiver requests and present recommended actions to the ARNG TPOC;

10. Adding, updating, and deleting system level user accounts for privileged access of government accounts; and

11. Removing dormant accounts based on business rules.

The contractor shall maintain a FISMA compliance with no CAT I (30 days to remediate), CAT II (60 days to remediate) and CAT III (90 days to remediate) vulnerabilities or have a government approved POA&M in place to mitigate findings within compliance windows (Exploitable vulnerabilities must be mitigated instead of placed on a POA&M). Vulnerabilities are not considered remediated until they are eliminated from the training and production environments.

The contractor shall update eMASS to reflect the status of security control and vulnerability scans.

The contractor shall be responsible for maintaining security control documentation, associating it to controls in eMASS and making it available upon request by the AO, ISO, ISSM, ISSO, or an outside agency.

The contractor shall monitor Authority to Operate (ATO) records for all SMMS/RCMS-G modules and support the Plan of Action and Milestones (POAM) as initiated by the Government. The contractor shall update eMASS instances to reflect system status.

Output: The contractor shall provide an in-process review of the Cyber Security and Compliance report to include a resolution POAM during each monthly technical status meeting (Reference C.5.1.2).

C.5.5 TASK 5 – HELP DESK / SERVICE DESK INFRASTRUCTURE

The contractor shall establish a service desk. (Reference Section J, Attachment H)

The Service Desk Infrastructure shall include:

1. Service Desk Ticketing System,
2. Service Desk Call Reporting System,
3. Service Desk Ticket Creation, and
4. Service Desk Managing Tickets.

The contractor shall provide Help Desk Verifiable Closed Tickets on a daily basis (Section F, Deliverable 33).

C.5.5.1 SERVICE DESK TICKETING SYSTEMS

This contractor-provided ticketing system shall be used to track and manage user inquiries as well as events reported though automated systems. In addition, the system must be able to track projects and their approval process.

System must generate the following minimum set of timestamps for each ticket record:

1. Create date and time;
2. Last updated date and time;
3. Resolved date and time; and
4. Closed date and time.

The Service Desk shall be located at the contractor’s facility.

The contractor shall provide and manage a ticketing system, which will be used to manage incident, problem and service requests reported by the users, SMMS/RCMS-G staff (Government and contractor), or automated sources.

To support service desk operations, the contractor shall provide:

1. Assistance with account issues;
2. Assistance with usage of the SMMS/RCMS-G Suite and its features;
3. Troubleshooting;

4. Coordination of resolution efforts; and
5. Grant access to the government program management team to perform reporting and analysis.

C.5.5.2 SERVICE DESK CALL REPORTING SYSTEM

Service Desk Call Reporting Requirements:

The contractor shall provide a Web-based reporting system capable of presenting current and historical data about call, email, and Web activities.

The contractor provided repository shall be capable of transmitting the above information to a standards based external database using SQL, Java Database Connectivity (JDBC), and/or Open Database Connectivity (ODBC) interfaces

The reporting tool shall have the flexibility to collect data and distribute reports via 'push' or 'pull' method, or a combination thereof.

The Call/Contact Type reports shall, at a minimum, include the following types of data for each call type:

1. Average and longest speed of answer;
2. Service levels;
3. Number of calls, offered, answered and abandoned;
4. For inbound calls (on a per hour, per 30 minute, and Busy Hour basis);
5. Average Speed To Answer;
6. Average Talk Time;
7. Average Wrap Up Time;
8. Average Hold Time;
9. Abandon Rate;
10. Longest Wait Time;
11. Longest Talk Time;
12. Number of received and associated response times for email and web requests;
13. Categorization of ticket priority as Critical, Normal, or Low; and
14. Additional statistics based on the individual handling the contact.

C.5.5.3 TICKET CREATION

The contractor shall use standard, compliant, database for storage of all tickets and supporting information. Support implementation of workflows associated with:

1. Escalation of tickets (automated assignment to an organization, or generation of alerts based on logically defined and time parameters);
2. Staff involved in the escalations and approval process must be alerted via email that an action is required within specified time frames; and

3. Support a hierarchical ticket classification scheme as specified in the contractor's SOP. Ensure all tickets that could impact Soldier pay or promotion be classified as critical.

The contractor shall ensure that each ticket record contains the minimum set of fields, which includes:

1. Type of ticket (incident, problem, request, etc.);
2. Work log (log of steps taken in resolving the ticket);
3. Each entry shall have a timestamp and ID of the person making the entry;
4. User's name, Military grade, and contact information;
5. Multi-level classification scheme;
6. Ticket Status; and
7. Assignment.

Ticket Creation Requirements: The SMMS/RCMS-G Service Desk is operated and maintained by the contractor and the contractor shall provide support to the users of the SMMS/RCMS-G Suite and its products. All calls from the users are routed to the Service Desk for initial handling. To handle incoming calls, the contractor shall:

Provide live telephone coverage from 8:00 am to 8:00 pm Eastern Time each weekday - Monday through Friday, excluding Federal holidays.

The contractor shall:

1. Answer calls and greet the customer with a standard welcome message as provided by ARNG;
2. Verify existing or obtain new user information;
3. Identify the nature of the problem and classify it correctly;
4. Record any additional information obtained from the user;
5. Assign priority as defined by service desk operations procedures; and
6. Provide the user with a ticket number.

To handle emails and Web submissions, the contractor shall:

1. Review email and Web request queues in regular intervals Monday through Friday 8:00 am to 8:00 pm Eastern Time, excluding Federal holidays. Requests that come in after close of business will be addressed starting at 0800 on the next business day;
2. Create tickets for each email and Web request; and
3. Contact user with ticket number.

Available statistics indicate an average call-length of seven minutes. Over a recent one-year period, the call distribution was as follows, this may or may not be similar to the actual call load, system outages and software changes may increase volume:

Time of Day of Ticket Creation	Number of Calls
8:00 am – 9:00 am	1,465
9:00 am – 10:00 am	1,548
10:00 am – 11:00 am	1,800
11:00 am – 12:00 pm	1,786
12:00 pm – 1:00 pm	1,496
1:00 pm – 2:00 pm	1,441
2:00 pm – 3:00 pm	1,387
3:00 pm – 4:00 pm	1,347
4:00 pm – 5:00 pm	988
5:00 pm – 6:00 pm	618
6:00 pm – 7:00 pm	51
7:00 pm – 8:00 pm	1
Total	14,385

Table 4 - Average Daily Service Desk Calls by Hour

C.5.5.4 MANAGING TICKETS

To manage tickets created by or assigned to the contractor, the contractor shall:

1. Maintain status of all open tickets and escalate as required;
2. Coordinate resolution with other internal and external teams, as appropriate;
3. Update the users with progress of the incident resolution through the ticket and; updates.

The contractor's staff shall own the problem resolution process from the initial contact with the users to resolution of the incident regardless of whether the problem is resolved within the Service Desk or it has to be escalated to other organizations. To ensure that the users are updated with the progress of the resolution process, the contractor's staff shall provide updates to the users on a regular basis. The contractor's staff shall also be responsible for verifying resolutions with the users, by doing regular checks with ticket submitters of a subset of resolved tickets, to verify user concurrence in the resolution. These checks shall take place on a monthly basis.

The contractor's personnel shall not reject a caller based upon a problem not being within their purview. The contractor shall make every effort to refer it to the most appropriate support organization. Support organizations may include external data partners, Cloud help desk, ARNG IT Help Desk, or other external support organization best suited to handle the caller's issue.

Support requests that have not been closed or have not had a defect resolution identified or been put in a hold status by the government after one month, must be grouped if multiple users are experiencing the same or similar issues and reported to the government with an explanation of the issue and the plan to resolve the issue within 30 days. All unresolved tickets after 30 days will be reported to the government as part of an extended resolution process.

Output: The contractor shall provide an in-process review of extended resolution tickets to include a resolution POAM during each monthly technical status meeting (Reference C.5.1.2).

C.5.6 TASK 6 – SMMS AND RCMS-G SYSTEMS OPERATIONS AND MAINTENANCE

The RCMS-G and SMMS systems are hosted in the ARNG Temple Jr. Army National Guard Readiness Center (TARC) in the Installation Processing Node (IPN) located in Arlington, VA.

The systems require varying levels of upgrade to become fully compliant. Some of the current projects that are in progress and are anticipated to be at least partially completed prior to award include:

1. MS SQL Server 2008 conversion to MS SQL 2016 - RCMS
2. Application and Shared component tool upgrades from legacy Adobe Flash to modern HTML5 – Various Applications (Almost 1 Million lines of code)
3. Server consolidation and compute/store increases - System
4. Test and Development environments migrated to a PII capable Cloud environment - System

C.5.6.1 SMMS/RCMS-G ENVIRONMENT

The contractor shall operate SMMS/RCMS-G at the designated host facilities in accordance with the IaaS table shown in Figure 1 (Section J, Attachment F). The IPN provides IaaS styled hosting environment for the physical infrastructure (racks, power, Local Area Network (LAN)/Wide Area Network (WAN), servers, firewalls, security devices, and other common services) and manages Virtual Machine (VM) servers hosting the SMMS/RCMS-G modules.

The contractor shall adopt and maintain administrative, technical, and physical safeguards and controls that are required for the security level and services being provided, in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time of contract award) found at: http://iase.disa.mil/cloud_security/Pages/index.aspx . Note: The new cyber incident reporting requirements of SRG section 6.4 become enforceable by the Government upon the effective date of the information collection governing the new reporting requirements (see DFARS case 2013-D018). However, this does not abrogate, limit, or otherwise

affect the contractor's obligation to comply with any other cyber incident reporting or other reporting requirement that is contained in this solicitation.

The contractor shall make all reasonable attempts to schedule planned maintenance outside of peak user hours (0800 EST through 2100 EST). When third party support is required to conduct maintenance, it may not be possible to schedule outside of these hours. However, off peak hours or non-business days should be considered as ideal planned maintenance windows for scheduling purposes.

The contractor shall perform maintenance necessary to respond to any Advisory, Conciliation and Arbitration Service (ACAS) scans run by host facilities.

The contractor shall comply with all Army Information Assurance Vulnerability Alerts (IAVAs) in regards to upgrades and scheduling of upgrades.

The contractor will coordinate with IPN and/or CSP to schedule Full and Differential backups of VMDK files. IPN will do file level backups/restores on all VMs including VM snapshots.

The contractor must manage Development, Test, Staging, and Production environments to ensure code is promotable to production with consistent results. It is the intent of the government to host all environments in the Cloud. Currently the vendor is responsible for hosting all environments other than production.

The TARC IPN provides (IaaS) support and maintains a virtualized hosting environment for the system, ensuring that the virtual infrastructure is available to the maximum extent possible. The contractor will be granted vCenter console access to view all VMware performance counters for their servers and have the ability to attach to the server console, reboot, shutdown, and turn off ARNG servers either directly or with IPN SA support.

The contractor shall maintain the SMMS/RCMS-G VMs at ARNG TARC IPN through proactive coordination with ARNG-G6 -- staff responsible for signal/computer management.

The contractor shall perform routine service and maintenance on a scheduled basis. Emergency maintenance for system operations will require support on a 24/7 basis. This maintenance shall be scheduled based on a minimal user interruption plan.

The contractor shall mitigate findings uploaded to the Vulnerability Management System (VMS), ensuring that all systems remain fully patched and are Army Information Assurance Vulnerability Alert (IAVA) compliant.

The contractor shall ensure that all systems remain fully DISA Standard Technical Implementation Guide (STIG) compliant. The contractor shall document in VMS or with a Memorandum for Record any STIG finding that cannot be mitigated stating why the finding cannot be applied and any mitigation in place to limit the vulnerability created by the STIG non-compliance.

Due to the need to comply with higher guidance from Network Enterprise Technology Command (NETCOM) and US Cyber Command the following permissions and clients will remain in effect for the system.

Domain Administrators and IMO IA personnel will remain in the local administrators groups on the servers. All personnel with access will maintain current training (IA, PII, HIPAA, etc.) prior to being granted access.

The contractor shall ensure Army Host Based Security System (HBSS), System Center Configuration Manager (SCCM), and Antivirus clients are installed and functional. It cannot be assumed that ARNG IPN support staff will be available on demand. Therefore, the vendor shall apply a continual monitoring approach and plan for the needed assistance so that all actions can be completed on time and with minimal interruption.

The contractor is responsible for backing up RCMS-G/SMMS systems and databases to the IMO provided backup Common Internet File System (CIFS) share using either the Microsoft provided tools, or third-party tools provided by the Government.

The contractor shall ensure backups are not encrypted or compressed in order to maximize the efficiencies gained by using the provided backup hardware.

The contractor shall monitor storage utilization and identify requirements for additional storage at least 2 weeks in advance.

The contractor shall coordinate with ARNG G6 and NETCOM to provide the required web proxy and filtering.

The contractor shall be responsible for ensuring annual Federal Information Security Management Act (FISMA) requirements are met. These requirements include annual system security assessment, annual test of security controls, and annual testing of the system's contingency plan.

The contractor shall operate RCMS-G/SMMS at the ARNG IPN hosting facility in accordance with the IaaS table shown as Figure 1 (Section J, Attachment F). RCMS-G consists of production elements (ARNG G1 data warehouse databases, RCMS-G modules and Web server) The ARNG TARC IPN provides IaaS styled hosting environment for the physical infrastructure (racks, power, Local Area Network (LAN)/Wide Area Network (WAN), servers, firewalls, security devices, etc.) as well as for the OS of the servers hosting the RCMS-G/SMMS modules.

The contractor shall maintain the RCMS-G/SMMS test system hosted at the ARNG TARC IPN/CSP to be consistent with the production environment.

The contractor shall prepare plans and execute the transition and/or integrate capabilities and data to other systems as directed by the Government while maintaining capabilities with minimal impact to users.

The contractor shall maintain the RCMS-G/SMMS virtual machines at ARNG IPN environment through a pro-active coordination with ARNG-G6 to ensure operational capability and security compliance.

In the event of a situation that impacts system availability, the contractor shall notify the TPOC as soon as possible after detection of the issue but not more than 12 hours after detection. Availability is measured 24/7/365 (excluding agreed upon maintenance windows) with a goal to have the system available 100% of the time.

C.5.6.4 WEB SERVER MAINTENANCE

The contractor shall maintain operational readiness of the Web servers (currently Apache and Internet Information Services (IIS)) that host the SMMS/RCMS-G and SMMS applications. There are currently five web sites hosted on the SMMS/RCMS-G server and three web sites hosted on the SMMS server. The support in this area includes the following tasks:
Ensuring web sites maintained under this contract continue to meet DoD security standards and maintain full accreditation in accordance with the security section of the Program Management Plan;

Ensuring public web sites are registered with the most popular search engines (e.g., Google Bing, Yahoo) to increase visibility, and take actions to ensure web sites private to the SMMS/RCMS-G program is hidden from those search engines;

Planning, coordinating, and conducting web site usability studies;

Ensuring public web sites are registered and take actions to ensure web sites are private to the SMMS/RCMS-G program;

Ensuring web sites, web applications, and data processes are secure and conform to the DoD Risk Management Framework;

Planning, coordinating and conducting web site usability studies and;

Providing a system capable of handling 6,000 concurrent visitors to the public site, conducting routine functions without system degradation.

The contractor shall provide a Web Server Maintenance Confirmation Report of completed maintenance tickets (Section F, Deliverable 25).

C.5.6.5 INCIDENT AND PROBLEM ANALYSIS

The incident/problem resolution process involves both immediate assistance with resolving problems and analyzing issues in order to prevent the recurrence of incidents and errors. To increase efficiency of employed systems and to minimize disruption to the on-going operations of SMMS/RCMS-G, the Government is driving the SMMS/RCMS-G program toward a more proactive approach to problem management. This approach relies on the ability to correlate and

analyze incidents and information from multiple sources including service desk tickets, change requests, alarms generated by automated sources and others. The goal of this approach is to identify potential problems before they actually occur and effectively improve customer service and system performance, while lowering support costs. The contractor shall implement a process to actively monitor activity and identify performance. This process will allow for problem analysis and product improvement recommendations.

The support in this area includes the following tasks:

- Performing analysis that leads to the identification of root cause of problems and the means of resolving them;
- Completing and submitting the root-cause analysis results, along with recommendations, to the Government for each major event (system warnings and exceptions as defined by the contractor's process), such as an event that results in an outage that cannot be resolved through standard procedure;
- Providing recommendations that are technical solutions and incorporate suggestions for improving internal processes and;
- Continually performing this analysis and presenting the Government with recommendations.
- Creating and managing a database that contains information about known problems and their expected resolution that is consistent with Information Technology Infrastructure Library's (ITIL®) Known Error Database approach and;
- Output: Presenting the summary results of the analysis, along with recommendations for improvement, as a part of the Monthly Status Report (Reference C.5.1.3 - Section F, Deliverable 04). The contractor shall provide an Incident and Problem Analysis Confirmation Report of Completed Tickets (Section F, Deliverable 26) Approximately 10,000 help tickets per year shall be expected.

C.5.6.6 ENGINEERING SUPPORT

The contractor shall provide engineering support to meet the changing needs of the SMMS/RCMS-G user community, maintain industry best practices, and plan for long-term growth and sustainability of the SMMS/RCMS-G Suite. The contractor shall identify potential projects to improve SMMS/RCMS-G capabilities and engineering changes needed to meet program objectives. The contractor shall perform additional engineering initiatives, to support changing technologies or are based on emerging requirements identified by the ARNG.

Engineering support shall include:

1. Providing technical improvement recommendations to ongoing SMMS/RCMS-G O&M efforts;

2. Anticipating changes in the SMMS/RCMS-G technical and business requirements and making recommendations implementing industry best practices;

3. Providing technical and business recommendations to support the SMMS/RCMS-G strategic planning process;

4. Assessing impact of changes to SMMS/RCMS-G requirements on technical and cost baselines;

5. Any changes or engineering support that become a requirement by a change in law, regulation, or policy that are not covered in the scope of this contract shall be; coordinated through the COR/CO for approval and contract modification

6. Providing ongoing coordination with software maintenance team(s) for tailored products, modules and models database and best practices support as provided by users to make engineering revisions;

7. Preparing, planning, and migrating hosting of the SMMS/RCMS-G and SMMS Development, Testing, and Production environments to a FEDRAMP approved DoD Cloud Service Provider (CSP) as directed by the government and;

8. Migrating capabilities into a common solution that provides a low code data driven software solution focused on providing support to all types of software maintenance such as

    a. Adaptive Maintenance
    b. Perfective Maintenance
    c. Corrective Maintenance
    d. Preventative Maintenance.

C.5.6.7 DEVELOP OPERATING LEVEL AGREEMENTS

Working with Other ARNG support contractors: ARNG employs services of multiple contractors and Vendors in support of its operations.

The contractor shall work with these entities and establish working agreements (e.g., OLAs) as needed that enable them to provide support that meets the requirements under this SOW.

ARNG will assist with coordinating the interactions between the SMMS/RCMS-G contractor and the other support contractors as needed.

There are approximately 50 contractors and other organizations that the SMMS/RCMS-G contractor shall:

1. Coordinate required to work with other contractors and Government organizations operating within the ARNG; and

2. Maintain and update agreements (Interconnect System Agreements, Memorandums of Agreement, OLAs, and Data Usage Agreements) as required with other contractors and Government organizations to ensure functionality with current and future military personnel systems.

C.5.6.8 CHANGE IMPLEMENTATION

The SMMS/RCMS-G is constantly changing and expanding. This expansion is primarily driven by: (a) availability of new data elements, (b) user requests, (c) technology evolution, and (d) ARNG mandates.

To support this expansion and changes, the contractor shall:

1. Provide technical resources and capabilities to change existing and implement new business logic and to update and change the SMMS/RCMS-G environment and its offerings;

2. Create and verify fields and metrics; and

3. Create new metrics (metadata and equations) to support new features, add new data sources or data versions, and make changes to SMMS/RCMS-G products.

4. The contractor shall be responsible for delivering the Configuration Management Plan within 15 days of task order award (Section F, Deliverable 31). The contractor shall demonstrate a working Configuration Management Database within 30 days of task order award (Section F, Deliverable 32). The contractor shall take the following precautions while engineering changes. Document dependencies as they become known;

    1. Create test scripts to test all changes. Test scripts may be manual or automated
    2. Exercise test scripts for all major components after any system deployment;
    3. Use Training Application for all tests before deployment to Production Application;
    4. Create system rollback points prior to implementing new changes;
    5. Advise the Government within 24 hours of a self-inflicted error and document the dependency to avoid future instances of creating the same error;
    6. Change work shall not begin without COR/TPOC concurrence;
    7. Change SMMS/RCMS-G functionality as mandated by DoD, Active Component, and ARNG manpower and human resource management policy changes;
    8. All changes shall follow the change management process. These solutions require implementation of good software change practices;
    9. Implement dual directional data interfaces between SMMS/RCMS-G and Integrated Personnel and Pay System Army (IPPS-A). Support data calls and testing of interface to IPPS-A system to ensure that the required system interfaces between SMMS/RCMS-G and IPPS-A provides accurate incoming and outgoing requirements; and
    10. Modify and optimize the SMMS/RCMS-G product, module, and model suite: Modify and optimize the SMMS/RCMS-G Suite to integrate with new operating systems, compilers, system utilities, and other system products as well as operate the Configuration Management process throughout the contract to include identification and labeling of configurable items, maintenance of configurable items, configuration verification and auditing with records auditable over time.

C.5.6.9 CONFIGURATION IMPLEMENTATION

An approved CR enters the Change Implementation process. The contractor shall implement changes to the system as identified in the Change Management process. To support Change Implementation the contractor shall:

1. Add, modify and delete code and business logic to implement changes;

2. Add, modify and delete data metrics in the data warehouse;

3. Add, modify and delete source code from a repository with branches dedicated branches for testing, development and production code;

4. Modify the system environment as required to implement change (inclusive of adding, modifying or deleting external data feeds);

5. Create test scripts for user acceptance testing;

6. Conduct user acceptance testing, regression testing, unit testing and other types of testing as required to implement the change;

7. Update system documentation after changes is implemented;

8. Summarize system changes completed on the Monthly Status Report (Reference Section C.5.1.2).

9. Maintain and change the SMMS/RCMS-G test strategy that includes unit, integration, system, and acceptance testing from both a top-down and a bottom-up approach. This strategy identifies data or software issues which, if not resolved, may threaten accuracy and operational status of SMMS/RCMS-G;

10. Develop and use System/Software Testing Checklists as outlined by the Software Test Plan to document testing of changes, or new developments. Testing shall include unit, integration, system, and acceptance testing from both a top-down and a bottom-up approach;

11. Test all changes prior to implementation to prevent the occurrence of any potential problems in products, modules, models, or systems and;

12. Maintain and report testing artifacts, including defect types, status, and resolution.

The ARNG will define specific change efforts based on information brought forward by internal and external stakeholders.

C.5.6.10 COOP SUPPORT

The contractor is responsible for and shall perform standard backups and software/data copies that support the ARNG providing and managing the COOP environment and equipment. To include troubleshooting and SMMS/RCMS-G specific SME support to the ARNG G6. The contractor shall provide an outline of the existing COOP Operations that identifies the existing process and potential weakness that the government should address. This plan shall be continually updated as the COOP procedures change or the environment changes (i.e., Cloud Migration) (Section F, Deliverable 27)

C.5.6.11 SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act requires Federal agencies to make their electronic and information technology (IT) accessible to people with disabilities. This applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology.

All electronic and information technology (EIT) procured through this task order must meet the applicable accessibility standards specified in 36 CFR 1194.2, unless an agency exception to this requirement exists. Any agency exceptions applicable to this task order are listed below.
The standards define Electronic and Information Technology, in part, as "any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The standards define the type of technology covered and set forth provisions that establish a minimum level of accessibility. The application section of the standards (1194.2) outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport, and production. This includes computers, software, networks, peripherals, and other types of electronic office equipment.

C.5.6.12 PROVIDE SMMS/RCMS-G TECHNICAL INFRASTRUCTURE LIAISON SUPPORT

The contractor shall provide dedicated and direct technical support to the ARNG IPN to plan and improve network and infrastructure posture. This will require individuals to have elevated system access and therefore an IAT II or higher qualification is required.

The dedicated IPN technical contractor shall provide support to:

1. Troubleshooting and repairing IAVA installation
2. Installing and troubleshooting security software (McAfee Products)
3. Troubleshooting and repairing backup access and replication activities
4. Performing required security scans
5. Security Technical Implementation Guide (STIG) management
6. Supporting internal CAB and other approval boards
7. Support to CCRI and ATO activities within the ARNG IPN

8. Provide general troubleshooting and repair of network and system level support to ensure system and network compliance

C.5.7 TASK 7 – APPLICATION AND FUNCTIONAL SUPPORT

The contractor shall identify and respond to defects or faults in the SMMS/RCMS-G Suite of applications, modules, performance or function. The contractor can expect approximately 320 corrective maintenance activities per year. Many application layer change requests can be completed by functional subject matter experts through meta-data updates utilizing the existing low code environment, thus requiring less involvement from traditional software developers.

The support in this area includes the following tasks:

- Producing and implementing a process to identify, track and resolve defects. This process shall include the development, test, and production environments with identification by Quality Control Testers, Meta-data managers, and/or Software developers, as well as field users;
- Defining a process to address high impact defects as well as routine defects;
- Ensuring that web applications are scalable to meet the future needs of the ARNG, and that applications make maximum practical use of object-oriented design and component reusability;
- Ensuring requirements identified in Attachment I for all SMMS/RCMS-G modules and applications are met;
- Tracking all defects as service desk tickets and updates information about their status and resolution;
- Providing the capability to identify and respond to inquiries of data abnormalities contained within SMMS/RCMS-G data source as it relates to historical data sources. Responses are required within 12 hours and;
- Providing the capability to inform Users when any module or application is offline or down for Maintenance or updates.
- The contractor shall provide a Defect Identification, Tracking and Resolution report, (Section F, Deliverable 44).

C.5.7.1 STANDARD REPORT GENERATION AND DISSEMINATION

The contractor shall ensure that all standard reports are generated, verified, and delivered to the recipients in a prearranged manner. Standard reports are recurring reports with the same data elements with format provided by the government (Section F, Deliverable 28). The majority of reports are available either as fixed reports or user defined ad-hoc reports, however, some reports are standard and recurring but are not available through an automated process and should be reviewed for potential automation within DPRO.

The contractor shall:

1. Use statistical sampling methods to verify accuracy of the reports;
2. Ensure that all reports and data files have been delivered by the agreed upon date and time;
3. Ensure that all pre-scheduled reports have run and can be accessed;
4. Ensure correctness of the reports in terms of format and integrity of data; and
5. Create raw data sets, using either manual or automated process, for delivery to recipients.
6. The contractor shall update standard reports monthly and upon request. All monthly reports are due NLT the10th calendar day of each month (if the 10th falls on a weekend/federal holiday, the report is due the last business day prior to the weekend/federal holiday). Complex data requests requiring the assistance of technical support will be initiated within 24 hours of receipt, and timelines for completion shall be maintained in accordance with the timelines developed during the change management process.

All reports must be completed/packaged according to the corresponding formats provided by ARNG, OUSD (P&R), DAPE-MP, regulatory and statutory guidance. At any time, OUSD (P&R) or DAPE-MP can change the format, reporting dates, or add or delete reports (Reference Section J, Attachment G).

C.5.7.2 AD HOC QUERIES AND REPORTS

The Government requires ad hoc queries and reports to be created each month. The tables below provide data on the number and structure of these queries and reports. The contractor is expected to produce 75-150 ad hoc queries per month (Section F, Deliverable 29). Each Ad Hoc Report shall be tested and verified before providing the report to the Government. The information shown is based on historical data; the size and structure of the queries and reports may vary in the future. Ad hoc reports are custom reports that cannot typically be created using the DPRO application, however, can lead to new DPRO reports or data metric creation that can be added to an established or new data-mart for consumption in the DPRO application. Many Ad hoc queries require an analyst that is an experienced user of Microsoft Excel, Power Point, and Microsoft SQL Server Management Studio. Data can be pulled from external and/or internal sources such as the SMMS/RCMS-G G1 Data warehouse to respond to an ad-hoc request.

Type of Effort	Workload (for Experienced SMMS/RCMS-G SQL Analyst)
Small	< 4 hours
Medium	4-24 hours
Large	> 24 Hours

Priority of Effort	Response Time
High	Less than 4 hour turn around
Medium	24 hour turn around
Low	96 hour turn around

Table 2 - Priority Levels for Ad Hoc Queries and Reports

C.5.7.3 CHANGE AND CONFIGURATION MANAGEMENT SUPPORT

Change Management focuses on how any change in the system is determined. The change management system incorporates activities such as identification of changes, impact analysis of changes, documentation of change requests (CRs), Change Control Boards (CCB), communications to stakeholders and implementations of approved CRs. All CRs require the TPOC's signature prior to entering the Change Implementation process. The Change Control Board is a government lead, contractor facilitated board that focuses on change management and scheduling.

Configuration Management focuses on how any change to the system should be performed. The Configuration Management Database (CMDB) is central to the process of Configuration Management. The CMDB includes information about the system's hardware and software as well as relationships between assets. The CMDB displays this information over time and can be used for activities such as root cause analysis, impact analysis, and Change Management.

C.5.7.3.1 CHANGE MANAGEMENT

The contractor shall be responsible for delivering the Change Management Plan within 15 days of time of task order award (Section F, Deliverable 30). The contractor shall operate the Change Management process throughout the contract to include Change Request collaboration and creation and management of the Change Control Board. The Contractor shall plan and conduct approved software releases at least once monthly, and meta-data updates at least weekly.

The SMMS/RCMS-G has three levels of changes to the application as described below:

Type of CR	Change Criteria	Estimated Number of Changes Annually
Minor Change Request (MCR)	Minor impact on requirements with no impact on infrastructure or environment. 5 Business Days to develop change management documentation and initial estimate	1,950

	(e.g., change in icon color, changing metric)	
System Change Request (SCR)	Minor to moderate impact on requirements with no impact on infrastructure or environment 15 Business Days to develop change management documentation and initial estimate (e.g., product changes, new report capability)	175
Engineering Change Proposal (ECP)	Moderate to major impact on requirements and may impact infrastructure or environment. 30 Business Days to develop change management documentation initial estimate (e.g., major system changes)	6

Table 3 - Type and Frequency of Change Requests

The contractor shall maintain a list of all applications in the SMMS/RCMS-G suite. (Application Owner Report, Section F, Deliverable 41). The contractor shall review all change requests and create an initial estimated change request classification.

Minor Change Request (MCR): Change requests that are determined to be a MCR shall be approved by the application owner.

System Change Request (SCR) or Engineering Change Proposal (ECP): Changes that are determined to be an SCR or ECP shall be approved at the CCB. Once the contractor has received approval for the SCR/ECP, the contractor shall provide the government an estimate of work hours that will be presented to the government. The government will determine if the estimate is complete and accurate and will accept or deny the estimate. Change Request Estimate (Section F, Deliverable 52). Once the estimate is approved, the work will be scheduled for a release. All change requests (MCR/SCR/ECP) will be scheduled and approved during the CCB. The contractor shall report as part of the IMRS the number and category of releases made each contract year and the cumulative over the life of the contract. This release schedule document will be considered the Integrated Master Release Schedule (IMRS) (Section F, Deliverable 42).

Emergency Changes: Emergency change requests shall be presented within 12 hours of contractor notification. The type of change request shall be determined, and if required an estimate shall be completed NLT the following business day. All emergency change requests will be reviewed during the weekly CCB to determine if the IMRS will need to be modified to accommodate the emergency change. If the work is so urgent that it must be addressed prior to the next scheduled CCB, then a special emergency CCB will be conducted to address only the

emergency change request and determine if a special release or patch must occur prior to the next scheduled release.

C.5.7.4 ANALYTICAL SUPPORT

The contractor shall provide analytical support for analysis of issues related to achieving and maintaining personnel readiness objectives and ad hoc responses to a wide range of complex questions raised by external and internal organizations.

The contractor shall make recommendations to the Government to most effectively integrate the diverse sources of data in SMMS/RCMS-G and to categorize/define the issues and problems that meet ARNG policy needs.

The contractor shall provide a limited number of personnel supporting analytics functions located at the Temple Army National Guard Readiness Center (TARC) located in Arlington, Virginia to provide analytical support services. This support averages 2-3 personnel per period of performance. The contractor assigned analysts shall:

- Apply objective, analytical, and orderly thinking to the analysis of complex operational and management problems, and supporting this analysis when appropriate with the use of tools and techniques such as statistical inference, models, mathematical programming, and simulations
- Conduct studies, research and prepare reports for executive level presentation
- Address specific data extraction and manipulation requirements including the ability to extract data from the G1 Data warehouse utilizing MS SQL Server Management Studio
- Identifying and formulating solutions to problems ranging from minor data quality issues to strategic forecasting of future personnel trends
- Conducting qualitative and quantitative analyses of complex military personnel and readiness issues
- Summarizing and synthesizing complex analyses into simplified terms for presentation to decision makers
- Integrating techniques into operational processes and algorithms used in the daily data preparation and quality control of the data warehouse
- Conduct Metadata analysis and modify metrics and workflows to establish greater accuracy and more automated functions.
- Provide results in a Monthly Ad Hoc Queries and Reports, (Section F, Deliverable 29)

C.5.7.5 PROVIDE SMMS/RCMS-G LIAISON SUPPORT

The contractor shall designate SMMS/RCMS-G liaisons of total staff for each SMMS/RCMS-G product, module, model, and prototype to interface with the ARNG POCs and user community. Each SMMS/RCMS-G liaison may handle multiple SMMS/RCMS-G products. Liaison support personnel should possess the ability to manage and define meta-data, extract application specific data utilizing MS SQL Server Management Studio, and provide regulatory and policy expertise to support the projects and applications in which they are supporting.

On a day-to-day basis, contractors serving as liaisons shall be responsible for:

1. Working with ARNG POCs to determine, recommend, prioritize and verify implementation of adaptation, maintenance, and change efforts;
2. Maintain continuous communication with ARNG POCs for program policy and implementation of the SMMS/RCMS-G products, modules, and models;
3. Convey requirements between government module functional owners and the contractor's program management team; and
4. Assist government functional module owners with the change management process.

Organization Supported
Strength Maintenance (HRR)
Human Resource (HRM)
Personnel Systems (HRP)
Personnel Policy (HRH)
Soldier and Family Support (HRS)

Table 5 - Liaison Support

C.5.7.6 SMMS AND RCMS-G SYSTEMS MAINTENANCE

The contractor shall maintain each of the SMMS/RCMS-G modules to ensure that they perform in accordance with the specified functional and performance characteristics as defined in the documentation for each module (Reference Section J, Attachment I).

The contractor shall:

1. Ensure the capability to upload, store and make edits to program policies;

2. Provide the capacities to view the definition of any code by hovering over the code with the mouse clicker;

3. Use common lookup tables where possible to minimize the number of locations requiring updates, update all lookup tables to conform to current policy and regulation. Lookup tables that are guided by regulation (MOS changes, and data codes standardized across the Army or DoD) shall be updated within five business days of the regulation change and shall take effect on the effective date of the regulation change;

4. Ensure access requests and approved use DD Form 2875 thru the User Management tool.

5. Add, Modify, and archive workflows to ensure system functions are compliant with current ARNG business functions.

6. Ensure the DD form 2875 (Section J, Attachment J) is updated annually (Section F, Deliverable 36); and

7. Add, modify and archive database metrics

SECTION D – PACKAGING AND MARKING

D.1 PRESERVATION, PACKAGING, PACKING, AND MARKING REQUIREMENTS

The contractor shall provide deliverables to addresses identified in Section G - Contract Administration in readable electronic format using Microsoft Office Suite and Adobe via email, unless otherwise specified. In addition, please refer to the Contract Deliverables table in Section F for Medium/Format.

The contractor shall use best commercial practices for formatting deliverables. Marking for Electronic Delivery. Electronic copies shall be delivered via email attachment to the TPOC, and GSA Assisted Services Shared Information System (ASSIST) Information Technology Support Services (ITSS) at portal.fas.gsa.gov. The contractor shall label each electronic delivery with the contract number and deliverable title in the subject line of the email transmittal.

D.2 MARKING OF REPORTS

All reports delivered by the contractor to the Government under this contract shall be delivered through ITSS (portal.fas.gsa.gov) and to the CO, CS, COR, and TPOC.

SECTION E – INSPECTION AND ACCEPTANCE

E.1 REQUIREMENTS SUMMARY

The intent is to ensure that the contractor performs in accordance with the defined requirements, that the Government receives the quality of products/services called for in the contract, and that the Government only pays for the acceptable products/services received.

The contractor, and not the Government, is responsible for the management and quality control actions to meet the terms of the contract. The role of the Government is to promote quality assurance to ensure standards are achieved.

The contractor's QCP (Section C.5.1.6) shall describe its method for measuring quality and plan for meeting service level agreement and delivery schedule.